NORTH DAKOTA

HOMELAND SECURITY

ANIT-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Water project to provide high-quality water to NW ND. A $110 million pipeline project will bring high-quality drinking water to areas of northwest North Dakota that desperately need it, officials said May 15. The Western Area Water Supply Project pipeline between Crosby and Wildrose will bring high-quality, treated drinking water from the Missouri River to residents of Burke, Divide, McKenzie, Mountrail, and Williams counties where water quality is poor and in short supply. The project is projected to serve as many as 75,000 people over the next 20 years. It will be primarily completed by the end of 2014. The loans that launched the project will be repaid by selling extra water to oil companies for hydraulic fracturing. Source: http://www.thedickinsonpress.com/event/article/id/58060/

Homes threatened by rising water at Rice Lake. Water has been rising at Rice Lake, a popular getaway a few miles southwest of Minot, North Dakota, leaving residents worried about how their lakeside homes will make it through the summer. Rice Lake sits above the Douglas Aquifer. The water level began rising more than a year ago after three consecutive winters of heavy snows. With no natural outlet to disperse heavy rainfall, the lake rose 8 inches in an 8-day period earlier in May, and it is currently rising about three-quarters of an inch a day, a resident said. A recent break in a portion of the Rice Lake sewer system is believed to have been caused by too much pressure from underground water. Rice Lake residents began a pumping program in the summer of 2011 that lowered the lake level, but it appears to have provided just a few months respite from the continual rise. A permanent solution being sought is a proposed $6 million pipeline leading south from Rice Lake into Douglas Creek. Source: http://bismarcktribune.com/news/state-and-regional/homes-threatened-by-rising-water-at-rice-lake/article_d684d096-9cb8-11e1-b4bd-0019bb2963f4.html

Regional

(Minnesota) **Minn. man targeted Mexican consulate.** A Minnesota man with suspected ties to white supremacist groups planned to attack the Mexican consulate in St. Paul, believing it would stir debate on immigration amnesty issues ahead of the 2012 Presidential election, according to a federal affidavit recently unsealed in federal court and obtained May 17 by the Associated Press. He was indicted in April on drug charges, though authorities had been watching him and another man since 2010 as part of a domestic terrorism probe. The affidavit said he had amassed weapons and wanted to attack minorities, people with left-leaning political beliefs, and government officials. “We consider him a threat, and we believe he had the capacity to carry these threats out,” an FBI spokesman said in an interview May 17. In the plot against the consulate, the suspect allegedly told an undercover agent he wanted to load a pickup truck with barrels of oil and gas, drive it into the consulate, allow the mixture to spill, then set it ablaze with a road flare. He also suggested placing hoax explosive devices along the May Day parade route in the Twin Cities, saying he had video of prior parades so he could identify parade participants. Source: http://www.google.com/hostednews/ap/article/ALeqM5gkvmdqt81Z6oQDfvNjf0pc21Ni_w?docId=10438384434541649560e247b00d8350

NATIONAL

Nothing Significant to Report

INTERNATIONAL

Nothing Significant to Report

BANKING AND FINANCE INDUSTRY

SEC charges China Natural Gas, chairman with fraud. A China-based natural gas company and its chairman were charged with fraud by the U.S. Securities and Exchange Commission (SEC) for concealing loans designed to benefit the chairman's family. In January 2010, the chairman and former chief executive (CEO) of China Natural Gas Inc. (CNG) arranged for two improper loans totaling $14.3 million, and then lied about them to the company's board, investors, and auditors, the SEC said May 14. According to the SEC, the former CEO concealed a $9.9 million loan made through a sham borrower to a real estate firm owned by his son and nephew. It said he also concealed a $4.4 million loan to Shaanxi Juntai Housing Purchase Co. The SEC said the CEO told CNG directors the loans involved senior Chinese government officers in charge of a liquid natural gas project, and "repeated this lie" to investors on a quarterly earnings conference call. It also said CNG did not properly report a $19.6 million acquisition made in the fourth quarter of 2008. The lawsuit seeks civil fines and a ban on the CEO from acting as an officer and director of a public company. In September 2011, CNG announced the CEO's resignation and said it would restate some financial results. Source: http://newsandinsight.thomsonreuters.com/Legal/News/2012/05_-_May/SEC_charges_China_Natural_Gas,_chairman_with_fraud/

Sophisticated bogus PayPal emails lead to phishing. PayPal users are being targeted with e-mails purportedly coming from the e-payment giant and asking for their help. The e-mail contains a link that will supposedly take users to PayPal's log-in page but lands them on a spoofed one. Once users "log in," they are asked to fill in personal and financial data, including name, birth date, phone number, home address; debit/credit card type, number, expiration date, and card verification number; Social Security number and two security questions and answers. Once submitted, this information is sent to the scammers who can use it to hijack the PayPal account and perform identity theft. Hoax-Slayer warns this scam is a bit more sophisticated than previous ones, as the text of the scam message is rather accurate, and the address of the fake Web site includes "paypal" along with a long string of numbers and letters. "The fake site includes all of the elements and navigation links familiar to PayPal users. However, clicking these links does not lead to another part of the site as expected but simply reloads the same scam form," a researcher pointed out. Source: http://www.net-security.org/secworld.php?id=12930&utm

P2P ZeuS variant used to steal debit card details. As revealed by security experts, Visa, MasterCard, Facebook, Gmail, Hotmail, and Yahoo all have a peer-to-peer (P2P) variant of the

Zeus platform in common, Softpedia reported May 15. For each platform, cybercriminals have made a clever scenario, Trusteer reported. When targeting Facebook users, attackers use a Web inject to push an offer that urges users to link their Visa or MasterCard debit cards to their social media account. By doing so, the victim allegedly earns cash every time he/she purchases Facebook credits. The attacks against Gmail, Hotmail, and Yahoo customers start with the advertisement of a new authentication service called 3D Secure, allegedly connected to the Verified by Visa and MasterCard SecureCode programs. The Hotmail scheme is somewhat similar with the potential victims being informed of the fact that "Windows Live Inc" is concerned about their security, offering a "100% secure, fast and easy" method of preventing fraud by linking the account to the debit card. In each scenario, the customer is presented with a number of textboxes in which he must enter his debit card number, expiration date, security code, and even the PIN. Source: http://news.softpedia.com/news/P2P-ZeuS-Variant-Used-to-Steal-Debit-Card-Details-269670.shtml

Treasury imposes sanctions on individuals linked to the Taliban and Haqqani Network. The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) May 17 designated two individuals pursuant to Executive Order (E.O.) 13224. A Haqqani Network communications official was designated for acting for, or on behalf of, a Haqqani Network commander and a Taliban financier was designated for providing financial support for, and or financial services to, the Taliban. The Haqqani Network commander was previously designated by the U.S. Department of State in May 2011 under E.O. 13224. The United States listed the Taliban as a Specially Designated Global Terrorist entity in July 2002. As a result of the May 17 actions, all property in the United States or in the possession or control of U.S. persons in which the two designated men have an interest is blocked, and U.S. persons are prohibited from engaging in transactions with them. Source: http://www.treasury.gov/press-center/press-releases/Pages/tg1584.aspx

Global Payments breach reportedly worse than expected. The security breach at credit card processing company Global Payments extends back further than was previously believed, H Security reported May 18. According to BankInfoSecurity, the incident is now thought to go back as far as January 2011 — it was originally believed to have taken place between January 21 and February 25, 2012, but was later dated to early June 2011. While initial reports of the breach suggested more than 10 million accounts were compromised, Global Payments later said fewer than 1.5 million card numbers were taken. Source: http://www.h-online.com/security/news/item/Global-Payments-breach-reportedly-worse-than-expected-1578956.html

Global Payments Breach fueled prepaid card fraud. Debit card accounts stolen in a recent hacker break-in at card processor Global Payments were showing up in fraud incidents at retailers in Las Vegas and elsewhere, according to officials from one bank impacted by the fraud. At the beginning of March, Danbury, Connecticut-based Union Savings Bank (USB) began seeing an unusual pattern of fraud on a dozen or so debit cards it had issued. When the bank determined the facility where the purchases took place was a customer of Global Payments, it contacted Visa to alert the card association of a possible breach, according to USB's chief risk

officer. That is when USB heard from a fraud investigator at Vons, a grocery chain in southern California and Nevada. According to the chief risk officer, the investigator said the fraudsters were coming to the stores to buy low-denomination prepaid cards, and then encoding debit card accounts issued by USB onto them. The thieves then used those cards to purchase additional prepaid cards with much higher values. The risk officer said Visa alerted USB that about 1,000 debit accounts it issued were compromised in the Global Payments breach — including the dozen or so card accounts that initially prompted USB to investigate. USB officials said the bank suffered about $75,000 in fraudulent charges, and that it has so far spent close to $10,000 reissuing customer cards. Source: http://krebsonsecurity.com/2012/05/global-payments-breach-fueled-prepaid-card-fraud/

Chemical and Hazardous Materials Sector

(Texas) **Suspicious packages found at chemical plant.** Four suspicious packages with a detonator marked "explosive" strapped to them were found at the INEOS Chocolate Bayou Plant in Brazoria County, Texas, May 15. The chemical plant's 900 contract workers were sent home for the day, but the 350 full-time employees remained at the plant. Federal and local officials investigated for 3 hours and deemed the plant to be safe. Officials said the packages were a pallet of paint that arrived at the plant in the morning. A detonator marked "explosive" was strapped to the shipment and wrapped in plastic. Investigators said they know who sent the paint and are questioning that person. According to its Web site, the plant manufactures olefins and polypropylene. Source: http://www.msnbc.msn.com/id/47432250/ns/local_news-houston_tx/

NRC prioritizes industry responses to request for post-Fukushima flood hazard evaluations. The Nuclear Regulatory Commission (NRC) updated part of its March 12 request for information from all U.S. nuclear power plants, setting out a schedule for completing flooding hazard re-evaluations recommended by the NRC's Near-Term Task Force, which examined lessons learned from the Fukushima Dai-ichi nuclear accident in Japan, said a May 11 NRC release. The prioritization schedule, outlined in a letter to every plant owner, gives plants 1, 2, or 3 years to complete the hazard evaluations. The evaluation results could lead to further assessment of potential flooding effects at the plants. Source: http://www.nrc.gov/reading-rm/doc-collections/news/2012/12-055.pdf

Man pleads guilty to stealing company's formulas. A scientist accused of stealing secret formulas from a Utah chemistry company pleaded guilty to a federal computer charge May 11. He entered the plea in U.S. District Court to one count of unlawful access to a protected computer, in exchange for prosecutors dropping 25 other charges against him. He had worked for North Logan-based Frontier Scientific Inc. from 2009 to 2011. He admitted to accessing a company chemical resource notebook and emailing the formula for meso-Tetraphenylporphine, or TPP, to his brother-in-law in India. Investigators say that relative was setting up a competing company to undercut Frontier Scientific on prices it charges for pharmaceutical chemicals. Frontier Chemical, which supplies chemicals for research and drug discovery, says no other

company in the world produces TPP in such large quantities. Source: http://www.foxnews.com/us/2012/05/12/man-accused-taking-trade-secrets-pleads-guilty/

Commercial Facilities

Communications Sector

Monster sunspot's solar flare strong enough to confuse satellites. An enormous sunspot unleashed a powerful solar flare May 16, triggering a radiation storm intense enough to interfere with some satellites orbiting Earth, space weather experts said. The flare erupted from monster sunspot complex AR 1476, which stretches about 60,000 miles from end to end, at 9:47 p.m. The flare spawned a class S2 solar radiation storm around Earth, said the Space Weather Prediction Center (SWPC), a branch of the U.S. National Oceanic and Atmospheric Administration. A SWPC description classifies S2 solar radiation storms as moderate, with the potential to cause infrequent "single-event upsets" in Earth-orbiting satellites. People aboard aircraft flying at high latitudes may also be exposed to elevated radiation levels during such events. The flare also caused limited radio blackouts on the sunlit side of Earth, SWPC researchers said, adding that the storm appears to be subsiding. Scientists described the May 16 eruption as a class M5, or intermediate, solar flare. Source: http://www.space.com/15736-monster-sunspot-solar-flare-satellites.html

ZTE confirms security hole in U.S. phone. ZTE, the world's fourth-largest handset vendor and one of two Chinese companies under U.S. scrutiny over security concerns, said one of its mobile phone models sold in the United States contains a vulnerability researchers said could allow others to control the device. The hole affects ZTE's Score model that runs on Google's Android operating system. The hole, or backdoor, allows anyone with the hardwired password to access the affected phone, a researcher for cybersecurity firm CrowdStrike said. ZTE and Chinese telecommunications equipment manufacturer Huawei Technologies were stymied in their attempts to expand in the United States over concerns they are linked to the Chinese government, though both companies denied this. Most concerns centered on the fear of backdoors or other security vulnerabilities in telecommunications infrastructure equipment rather than in consumer devices. Reports of the ZTE vulnerability first surfaced the week of May 14 in an anonymous posting on a code-sharing Web site. Since then, others alleged different ZTE models, including the Skate, also contain the vulnerability. The password is readily available online. ZTE said it confirmed the vulnerability on the Score phone, but denied it affected other models. The CrowdStrike researcher said his team analyzed the vulnerability and found the backdoor was deliberate because it was being used as a way for ZTE to update the phone's software. It is a question, he said, of whether the purpose was malicious or just sloppy programming. While security researchers highlighted security holes in Android and other mobile operating systems, it is rare to find a vulnerability apparently inserted by the hardware manufacturer. Source: http://www.reuters.com/article/2012/05/18/us-zte-phone-idUSBRE84H08J20120518

Critical Manufacturing

52,000 Acuras recalled for steering loss, fire risks. Acura announced the recall of 52,615 TL sedans from the 2007-08 model years because of a faulty power steering hose, USA Today reported May 17. In the affected vehicles, the hose may deteriorate over time and leak fluid. That could lead to a loss of steering control. If power-steering fluid leaks onto the catalytic converter, it could start a fire. The recall will begin in June, and dealers will replace the hose. Source: http://content.usatoday.com/communities/driveon/post/2012/05/52000-acuras-recalled-for-steering-loss-fire-risks/1#.T7ZiKlIvDzD

Defense/ Industry Base Sector

U.S. defense secretary restricts F-22 flights due to oxygen system complaints. May 15, the U.S. Secretary of Defense ordered the Air Force to restrict flights of its new F-22 stealth fighters because of continuing problems with the aircraft's oxygen system. At least 22 pilots have suffered from oxygen deprivation while in flight since April 2008. The secretary ordered that all F-22 flights remain within a "proximate distance" of an airfield in case a pilot should suffer from a hypoxia event and be forced to land. That will force an immediate end to F-22 patrol missions over Alaska. The secretary also ordered the Air Force to accelerate installment of a backup oxygen system in all F-22s and provide monthly progress reports on efforts to identify the problem with the current oxygen system. The Air Force does not expect to begin installing automatic backup oxygen systems until December. Source: http://www.firstcoastnews.com/news/article/256711/6/Panetta-Restricts-F-22-Flights-Due-to-Oxygen-System-Complaints

Emergency Services

(Maine) **Radio jamming again a problem in York County.** Authorities thought the threat of a federal investigation finally stopped the person jamming Maine's York County emergency radio transmissions, often delaying responses, but after several weeks without a problem the mystery jammer is apparently back at work. The Lebanon fire chief said the latest incident occurred May 12 as firefighters called for mutual aid to battle a mobile home fire in Lebanon. Firefighters were unable to communicate with dispatchers. The chief said response was delayed by 5 to 10 minutes. The mobile home was destroyed, and three others nearby were damaged. Source: http://www.seacoastonline.com/articles/20120515-NEWS-120519853

Energy

(Vermont) **Vermont becomes first State to ban fracking.** Vermont became the first State to ban the controversial natural gas drilling practice known as hydraulic fracturing, or fracking, NewsCore reported May 17. However, the law will have no immediate effect — Vermont does not have any drilling projects underway, and there is no information to suggest the State has underground gas reserves that could be tapped by fracking. The Vermont law also bans the importation and storage of wastewater associated with fracking. The drilling tactic involves the

high-pressure injection of a mixture of water and chemicals deep underground to blast shale rock to release natural gas. Source: http://www.myfoxphilly.com/dpps/news/vermont-becomes-first-state-to-ban-fracking-dpgonc-20120517-fc_20009541

Food and Agriculture

Preliminary FDA inspection report cites flaws at Diamond Pet Foods plant. Diamond Pet Foods, the company behind a massive recall of dry dog food due to Salmonella contamination that sickened at least 16 people, was not taking "all reasonable precautions" to ensure the safety of its product, according to a U.S. Food and Drug Administration (FDA) inspection report. The report, posted by the FDA May 15, was the result of a week-long inspection that began April 12 after an outbreak of human Salmonella Infantis infection was traced to contaminated pet food manufactured at the Diamond Pet Foods plant in Gaston, South Carolina. The report stated Diamond was using cardboard and duct tape on some equipment, and there were damaged paddles on the conveyor. The inspectors also noted some surfaces at the facility were encrusted with food residues. As of May 11, at least 15 people in 9 states and 1 person in Canada were confirmed infected with Salmonella from contact with the contaminated dry dog food or from contact with a pet that had eaten the tainted product, according to the Centers for Disease Control and Prevention. Diamond Pet Foods recalled nine brands of dry pet foods manufactured at its Gaston plant between December 9, 2011 and April 7. Several other companies whose food was also produced in the facility joined the recall. Source: http://www.foodsafetynews.com/2012/05/preliminary-fda-inspection-report-cites-flaws-at-diamond-pet-foods-plant/

(Colorado; Iowa) **Colorado issues quarantine for horse virus.** The Colorado Department of Agriculture quarantined a Douglas County ranch after confirming one case of a potentially fatal horse virus, the Davenport Quad-City Times reported May 15. State officials said the horse was brought to Colorado from Iowa and was euthanized after showing signs of the disease. State agriculture officials said the latest equine herpes virus case was not associated with a show or event like the one blamed for a serious outbreak in 2011. Infected animals usually get sick between 2-14 days after they are exposed to the virus. Source: http://qctimes.com/news/state-and-regional/iowa/colorado-issues-quarantine-for-horse-virus/article_c93dea87-f202-5fb9-8335-4d357d21a5b7.html

Virus sparks quarantine on B.C. salmon farm. British Columbia's salmon farming industry is on high alert after the discovery of a lethal fish virus at one farm on the west coast of Vancouver Island, CBC News reported May 18. The Canadian Food Inspection Agency has quarantined the farm at Dixon Bay, north of Tofino. Mainstream Canada, which runs the operation, said it would destroy its entire stock of 560,000 salmon to prevent the disease from spreading. The company said Infectious Hematopoietic Necrosis (IHN) was detected during routine testing May 14. "So we are just going to depopulate," Mainstream's spokesperson said, adding, "we will lose money. It's in the millions." A fish pathologist for the B.C. Ministry of Agriculture concluded the farmed fish were infected by wild salmon which carry IHN, but have developed resistance to the virus. He said IHN is present in most wild salmon consumed at the dinner table, but is

harmless to humans. It is deadly, however, to Atlantic salmon raised in open-net pens in the Pacific Ocean. Source: http://www.cbc.ca/news/technology/story/2012/05/17/bc-salmon-farm-quarantined-lethal-virus.html

FDA halts shellfish imports from Korea. The Food and Drug Administration (FDA) stopped the shipment of fresh and frozen oysters, clams, mussels, and scallops from Korea to the United States because many of these molluscan shellfish may be contaminated, according to a news release from the Washington State Department of Health. The action comes with removal of all certified dealers in the Korean Shellfish Sanitation Program from the FDA's Interstate Certified Shellfish Shippers List, the health department stated, according to a May 12 report from Food Safety News. As a result, the Washington State Department of Health is advising consumers not to eat any fresh or frozen shellfish from Korea and is working with distributors and local health agencies to recall such products. Source: http://www.foodsafetynews.com/2012/05/fda-halts-shellfish-imports-from-korea/

Government Sector (including Schools and Universities)

IG finds gaps in TSA reporting of security breaches. Only about 4 out of 10 security breaches involving unauthorized access at airports are reported to the Transportation Security Administration's (TSA) central performance database, according to a new audit. The acting inspector general (IG) at the DHS testified on the gaps in reporting to the House subcommittee on transportation May 16. He presented the results of his office's recent investigations of security breaches involving unauthorized access at U.S. commercial airports. Those breaches are defined as incidents in which one or more people gain access to a protected-access area of the airport without being screened or inspected under the TSA's standard operating procedures. The TSA documents the breaches at each airport, and TSA staff is supposed to forward the documents to the agency's central database. The audit showed inconsistent reporting. "We determined that only 42 percent of the security breaches we reviewed in individual airport files were reported in TSA's official record," the IG said. The audit also found corrective action was taken for only 53 percent of the breaches reviewed. The IG also mentioned a related audit that found other gaps in security at the airports, including incomplete vetting and verifications of employee identification information. Source: http://fcw.com/articles/2012/05/16/tsa-reporting-gaps.aspx

Influential panel calls for steep reduction of U.S. nuclear weapons. An influential panel is calling for an 80 percent reduction of U.S. nuclear weapons and an elimination of all nuclear armed intercontinental ballistic missiles, the Associated Press reported May 16. A report for the advocacy group Global Zero argues that the United States needs no more than 900 total nuclear weapons for its security in a post-Cold War world. The Presidential Administration is reportedly considering at least three options for lower total numbers of deployed strategic nuclear weapons: reducing their numbers to 1,000 to 1,100; 700 to 800; or 300 to 400. The Global Zero report calls for such weapons to be reduced to about 450, while maintaining an equal number

of stored weapons. The proposal also calls for achieving the cuts over 10 years. At a time of tight defense spending, the authors also estimate that the cuts would save the U.S. $100 billion over a decade. Source: http://www.foxnews.com/politics/2012/05/16/influential-panel-calls-for-steep-reduction-us-nuclear-weapons/

(Washington) **Suspicious package outside Wash. justice center.** A Benton County sheriff's officer said a package left outside the justice center May 14 in Kennewick, Washington, was made to look like a bomb with black tape and a pipe but had no explosive device. He said the package was filled with screws. It was blown up by the Richland bomb squad. Informational pickets spotted the package. Part of the building was evacuated. Source: http://www.thenewstribune.com/2012/05/14/2144851/suspicious-package-outside-wash.html

Anonymous claims access to classified U.S. databases. A hacker affiliated with Anonymous claims the collective has access to U.S. classified databases, TG Daily reported May 14. The hacker faces 15 years in prison for assaulting the county Web site of Santa Cruz, California, and is currently hiding out in Canada to avoid prosecution, courtesy of what he describes as a new "underground railroad," or a network of safe houses across the country. He told Canada's National Post that the collective has access to "every classified database" in the U.S. government. According to the hacker, the digital keys were handed to Anonymous operatives by the same "people who run the systems." He emphasized it was only a matter of time before the collective chose to disseminate database contents. "Now people are leaking to Anonymous and they're not coming to us with this document or that document or a CD, they're coming to us with keys to the kingdom, they're giving us the passwords and usernames to whole secure databases that we now have free reign over," he added. Source: http://www.tgdaily.com/security-features/63368-anonymous-claims-access-to-classified-us-databases

(Maryland) **Talbot school assault plan foiled.** The Talbot County, Maryland sheriff's office said Easton High School in Easton was the target of a planned attack by a current student, WBOC 16 Salisbury reported May 15. The plan was extensive, according to police, and would have allegedly involved the use of bombs and firearms to attack the building, students, and faculty. Parents were notified by voice message of the alleged plot 2 weeks after the arrest was made. The sheriff's office said the student was released to the custody of his family and was being monitored by a GPS ankle bracelet. Source: http://www.wboc.com/story/18382176/talbot-school-assault-plan-foiled

UGNazi hackers leak data from Washington Military Department. UGNazi hackers breached the site of the Washington Military Department and leaked data from the Web site's databases. The hackers leaked name servers, MX records, and the names and IP addresses of the subdomains used by the State of Washington. They also leaked around 16 user account details, consisting of usernames and password hashes, including the ones of the site's administrator. "This is just a continuation of our attack against wa.gov, but other than that, like we said we're not done with the government or anyone to be exact," a hacker told Softpedia. Source:

http://news.softpedia.com/news/UGNazi-Hackers-Leak-Data-from-Washington-Military-Department-269244.shtml

Information Technology and Telecommunications

Security vulnerability in sudo's netmask function patched. The developers of sudo released updates to the privilege elevating utility to patch a bug that allows an attacker to execute commands they should not be able to access on a remote system. Shortly after, they issued a regular update that includes these fixes along with several new features. Sudo versions 1.8.4p5 and 1.7.9p1 fix a security issue in the program that can allow a legitimate user who is included in the sudoers file to run commands on other hosts. When sudo is asked to run a command by a user, it consults sudoers to see if the user has permission. Sudoers rules include the ability to define permission by the host's IP address by matching with absolute addresses or matching with a netmask specification. It is the matching with netmasks, which are typically used to allocate users permissions by subnet, where the problem lies. The flaw is present in the IP network matching code of sudo versions 1.6.9p3 through 1.8.4p4. The exploit was reported internally through Red Hat's Bugzilla bug tracking system and was already fixed in Ubuntu by backporting the fix to older versions of the package. Red Hat is also expected to fix its versions of sudo soon. The project advised all users to update to a patched version of the program as soon as possible. Where they cannot upgrade, users are advised to switch to defining host permissions using IP addresses instead of netmasks. Source: http://www.h-online.com/security/news/item/Security-vulnerability-in-sudo-s-netmask-function-patched-1578395.html

Pinterest scam toolkits widen the pool of potential scammers. Pinterest scam toolkits are available for sale to inexperienced scammers, according to McAfee. Usually sold on underground forums, these toolkits contain many tools. All actions needed to scam users are included and automated: creating Pinterest invites and mass comments on posts, mass creation of bit.ly links, and scraping Amazon for products based on given keywords and then submitting them to Pinterest. Pinterest scams usually work by luring people in with offers of free gift cards, and the offered links land them either on sites hosting survey scams, on Amazon or other sites (which results in the scammers earning money by referral), or lead them to premium rate trojans (if the Pinterest visitor uses a mobile device to visit the site). Source: http://www.net-security.org/secworld.php?id=12931&utm

Popular surveillance cameras open to hackers, researcher says. Three of the most popular brands of closed-circuit surveillance cameras are sold with remote Internet access enabled by default, and with weak password security — a classic recipe for security failure that could allow hackers to remotely tap into the video feeds, according to new research. The cameras, used by banks, retailers, hotels, hospitals, and corporations, are often configured insecurely — thanks to these manufacturer default settings, said a senior security engineer at Gotham Digital Science. As a result, he says, attackers can seize control of systems to view live footage, archived footage, or control the direction and zoom of adjustable cameras. The researcher and his team were able to view footage as part of penetration tests they conducted for clients to

uncover security vulnerabilities. Source: http://www.wired.com/threatlevel/2012/05/cctv-hack/

NCC Group maps source of global hack attempts during Q1. Using data collected from DShield, the NCC Group mapped out its latest report on the origin of computer hacking attempts for the first quarter of 2012. NCC noted the top 10 changed significantly since its previous report 3 months ago. Italy, France, and India dropped off the top 10 list, while the Ukraine in fifth, South Korea in ninth, and the United Kingdom made the list. Russia showed a large increase, with more than 12 percent of global hacks originating from the country, putting it in third place, behind the United States and China. There was also a rise in hacks appearing to originate from the Netherlands, up from 3.1 percent to over 11 percent, moving it into fourth place in the hacking chart. Source: http://www.securityweek.com/ncc-group-maps-source-global-hack-attempts-during-q1

Spam with malicious attachments rising. While the volume of spam messages is falling, the number of messages containing malicious attachments increased, meaning spam is growing more dangerous even as it becomes less prevalent, according to a Bitdefender study. The number of malicious attachments in January 2012 rose 4 percent from the same period in 2011, even as the overall number of spam messages sent dropped by more than 16 percent in the first quarter of 2012 from the last quarter of 2011, Bitdefender research shows. Of the 264.6 billion spam messages sent daily, 1.14 percent carry attachments — about 300 million of which are malicious. After increasing in January, the growth of malicious attachments leveled-off amid an apparent pause in spam campaigns even though spam continued to fall overall. Attachments may come in the form of phishing forms that trick users into typing in credit card credentials for scammers to use whenever they want. Or, they may pack malware such as trojans, worms, and viruses that can eventually cause trouble for users. Source: http://www.net-security.org/malware_news.php?id=2113&utm

CERT warns on critical hole in SCADA software by Italian firm Progea. The DHS issued a bulletin May 10 warning about a previously undisclosed, critical vulnerability in Movicon 11, a product used to manage critical infrastructure including the manufacturing, energy, and water sectors. The Industrial Control Systems Cyber Emergency Response Team posted an advisory that warned customers of Progea Srl that a memory corruption vulnerability in the Movicon Human Machine Interface software could allow a remote attacker to knock Movicon devices offline using a specially crafted HTTP POST request sent to the Movicon OPC server component. Progea issued a fix for the problem. Source: http://threatpost.com/en_us/blogs/cert-warns-critical-hole-scada-software-italian-firm-progea-051112

Avast warns about "FakeInst" and alternative Android markets. The large number of malicious Web sites designed to infect Android devices with the Android:FakeInst SMS trojan made Avast security experts issue another warning to alert users. They advise smartphone owners to beware of fake-looking alternative Android application markets. Researchers found several domains, such as t2file(dot)net and uote(dot)net, which store at least 25 new apps that mask the piece of malware. After users are lured onto these Web sites, they are presented with a

phony Downloader program. This app tells the victim the operation may cost money, but the Quit button does not work. Once the installation process begins, there is nothing a user can do except click on the Agree or OK buttons. Once one of these options is selected, an SMS to a premium rate number is sent out. The trojan contains premium numbers for about 60 different countries worldwide. In order to prevent experts from analyzing the malware, its creators used AES encryption to make the file inaccessible. Source: http://news.softpedia.com/news/Avast-Warns-About-FakeInst-and-Alternative-Android-Markets-269380.shtml

Fuzz-o-Matic finds critical flaw in OpenSSL. Codenomicon helped identify a critical flaw in widely used encryption software. A flaw in the OpenSSL handling of CBC mode ciphersuites in TLS 1.1, 1.2, and DTLS can be exploited in a denial-of-service attack on both client and server software. The flaw was found with Fuzz-o-Matic, a cloud-based testing platform. The TLS security protocol is the current Internet standard for encrypting and authenticating application traffic. TLS is used by millions of people every day in online banking, e-commerce, e-mail, and Voice-over-IP applications. The OpenSSL is an open-source implementation of TLS and is employed in standard operating systems, Web browsers, e-mail clients, and network devices ranging from WiFi access points and DSL modems to industrial-strength core routers. Source: http://www.net-security.org/secworld.php?id=12916&utm

National Monuments and Icons

Mowing halted at national parks after fatal fall. Mowing at all national parks has been suspended indefinitely because of safety concerns after a maintenance worker cutting grass along the Blue Ridge Parkway in North Carolina fell to his death, the Associated Press reported May 15. The National Park Service sent an order to its regional offices May 11 to halt mowing at its 397 parks that are spread across every state except Delaware. The seasonal worker's riding mower fell more than 140 feet down a boulder-strewn embankment May 7. It is unclear how long the grass will grow unchecked nationwide. A NPS spokesman said each park has a safety review checklist to complete before mowing can resume. The duration of the suspension will depend on the size of the park, the amount of equipment, and the number of employees. Source: http://www.kgwn.tv/story/18426074/mowing-halted-at-national-parks-after-fatal-fall

(Arizona) **Northern AZ wildfire grows, prompts evacuations.** Firefighters battled a growing wildfire May 14 in northern Arizona that forced residents from their homes in a historic mining town. The fire in Crown King began on private land May 13 and grew to more than 4.5 square miles, destroying two buildings and one trailer, said a Prescott National Forest spokeswoman. The fire started at a "structure" and was human-caused, she said. The area remained under a mandatory evacuation order, though a Yavapai County sheriff's spokesman said in a news release that most of the town's 350 residents chose to stay in the community of mostly summer homes. The American Red Cross reported five evacuees at a shelter in Mayer. Five wildfires in the State charred more than 9 square miles by late May 13. Billowing smoke from the fire and another one to the west near Crown King could be seen in Phoenix, more than 50 miles south. The fire overtook part of Crown King Road, making the road to the town inaccessible, a sheriff's office statement said. The State's other large fire, in an area 120 miles

east of Phoenix, was spotted in Tonto National Forest, where it burned about 4 square miles. That blaze was about 20 miles south of Payson, a gateway town to mountains popular among Arizona campers. The fire was moving northeast toward a wilderness area, a Tonto National Forest spokesman said. Crews were also at a blaze believed to be sparked by lightning on the Fort Apache Indian Reservation in eastern Arizona, which charred more than 480 acres. Source: http://www.foxnews.com/us/2012/05/14/arizona-wildfires-keeping-crews-busy/

Postal and Shipping

(Massachusetts) **Hazmat crew removes suspicious parcel from Dighton Post Office.** A HAZMAT crew responded to the Dighton, Massachusetts Post Office and removed a suspicious piece of mail May 14. Postal workers called emergency responders after discovering a powdery substance on a piece of mail, according to the Dighton Fire Department. The Massachusetts Department of Fire Services sent two men wearing HAZMAT suits into the post office to remove the parcel. A postal truck was also cordoned off. The Dighton fire chief said the department was waiting for results from the State laboratory. In addition to the Department of Fire Services, an agent from the FBI and a postal inspector responded. The post office was closed for the day. While the questionable parcel was in the building, the postal truck that carried the mail was cordoned off by the HAZMAT crew, a Dighton selectman said. "The truck went off and delivered mail to about 50 or 60 houses," he said. "The powder was all over the truck. When they brought it back to the post office, that's when they called the HAZMAT." Source: http://www.tauntongazette.com/topstories/x255395046/Hazmat-crew-removes-suspicious-parcel-from-Dighton-Post-Office

US Postal Service will not ship electronics with lithium batteries abroad, citing safety risks. The U.S. Postal Service is banning international shipments of electronics with lithium batteries such as smartphones, laptops, and iPads, citing the risk of fire. Beginning May 16, consumers may no longer make the shipments, including to army and diplomatic post offices. That means friends and family will have to use more expensive private companies such as UPS and FedEx to ship electronics to U.S. troops based abroad. The Postal Service cited discussion by the International Civil Aviation Organization and the Universal Postal Union. They issue semi-binding guidelines for global trade. Officials expect that U.S. consumers can resume shipments in most cases after January 1, 2013, once the agency develops a new policy "consistent with international standards." Lithium batteries are believed to have caused at least two fires on cargo planes since 2006. Source: http://www.washingtonpost.com/politics/us-postal-service-will-not-ship-electronics-with-lithium-batteries-abroad-citing-safety-risks/2012/05/11/gIQAgCsaIU_story.html

Public Health

90% of surgery centers experiencing drug shortage at least weekly. Almost 90 percent of surgery center respondents are experiencing a drug shortage at least weekly, according to an ASC Association drug shortage survey, Becker's ASC Review reported May 15. In addition, more than 80 percent of respondents were never given advanced notice of the drug shortage. The

survey found that half of respondents had to use an alternative level of sedation and/or alternative medications because of a drug shortage, which many respondents said led to an increase in patient nausea and vomiting. Over 10 percent of responding facilities had to reschedule a procedure due to a drug shortage, according to the survey. Source: http://www.beckersasc.com/anesthesia/90-of-surgery-centers-experiencing-drug-shortage-at-least-weekly.html

(Kentucky) **University Hospital on heightened security following Louisville shootings.** Police cars packed the emergency room entrance at University Hospital after multiple shootings in Louisville, Kentucky, left three people dead May 17. As ambulances began arriving to University Hospital with several other shooting victims, officers also began arriving to heighten security. Multiple people and employees entering and leaving the hospital said some doors were locked and security was standing at certain doors, checking people who entered and exited the facility. Hospital officials say, however, the hospital was not officially on lockdown, and there were ways to enter and leave the hospital. Source: http://www.wdrb.com/story/18516391/university-hospital-on-heightened-security-following-louisville-shootings

TRANSPORTATION

NHTSA unveils proposed stability control mandate. The National Highway Traffic Safety Administration proposed a first-ever federal motor vehicle safety standard to require electronic stability control (ESC) systems on large commercial trucks and buses, Truckinginfo reported May 16. The rule would affect vehicles with a gross vehicle weight rating of more than 26,000 pounds. As proposed, the rule would take effect between 2-4 years after the standard is finalized, depending on the type of vehicle. The proposal also includes standards for performance testing of the technology. Agency research shows the technology could prevent up to 56 percent of rollover crashes each year, and another 14 percent of loss-of-control crashes. Source: http://www.truckinginfo.com/news/news-detail.asp?news_id=76971

FAA moves on integrating drones into U.S. airspace. May 14, the Federal Aviation Administration (FAA) implemented rules that allow a government public safety agency and first responders to operate drones weighing 4.4 pounds or less in the U.S. air space, but under certain restrictions: these drones should be used for training and performance evaluation, they must be flown within the line of sight of the operator, less than 400 feet above the ground, during daylight conditions, inside Class G (uncontrolled) airspace, and more than 5 miles from any airport or other location with aviation activities. The FAA said if safety agencies then apply for a waiver, the agency will allow the operation of drones weighing up to 25 pounds. The FAA said it has been working to ensure the safe integration of unmanned aircraft systems (UAS) in the U.S. National Airspace System (NAS). Already, the agency said it achieved the first unmanned aircraft systems milestone included in the 2012 FAA reauthorization bill — streamlining the process for public agencies to safely fly UAS in U.S. airspace. Federal, State, and local government authorities must obtain an FAA Certificate of Waiver or Authorization (COA) before flying drones in the national air space. Source:

http://www.homelandsecuritynewswire.com/dr20120516-faa-moves-on-integrating-drones-into-u-s-airspace

(Washington) **Copper cable worth $250K stolen from rail tunnel.** Sound Transit officials in Washington State said someone stole about 70,000 pounds of valuable copper cable from a tunnel inside the elevated light rail track between SeaTac and Seattle. A transit agency spokesperson said May 11 that the missing cable poses no danger to trains or passengers. He said the cable protects the structure from any stray currents. Source: http://seattletimes.nwsource.com/html/localnews/2018192463_apwacoppertheft.html

CSX recently launched a free, online training program to educate emergency personnel on how to safely respond to incidents on and around railroad property and equipment. The site at www.csxsafe.com is the first of its kind launched by a U.S. railroad for this audience. CSXSAFE offers participants the opportunity to gain an understanding of how railroads operate, including some of the hazards of working around the rails and necessary protocols to keep responders safe. This web-based program takes less than an hour to complete, and is intended to provide important information to public agency personnel in fire and police departments, rescue and emergency medical organizations. "Every day, emergency workers put themselves in harm's way to protect the public in homes, office buildings, factories, agricultural facilities and other locations, each with distinct hazards," said Mike Lunsford, CSX director-chemical safety. "CSXSAFE is one of the ways we help these brave men and women by educating them on the unique challenges posed by railroad operations. Emergency personnel have to know a great deal about a variety of different industries and settings, and we want to make it as easy as possible for them to learn about ours." The educational section of the site is organized into four parts, providing basics on Safety, CSX Operations, Initial Response and Railroad Equipment. Upon completion of the training modules, participants take a quiz, print a certificate of completion and are able to browse through upcoming in-person training opportunities being offered across the CSX network. "For those who don't work for the railroad, our equipment can be intimidating and some safety risks may not be apparent," said Cliff Stayton, director of Community Affairs & Safety. "This training is designed to help emergency workers make good decisions quickly and know who to call to get help."

Water and Dams

(Massachusetts) **Alarm over evidence of dam tampering.** The Ayer, Massachusetts, Conservation Commission was alarmed to find evidence of human tampering with a critical upstream beaver dam within the Pine Meadow conservation land, Nashoba Publishing reported May 18. “Someone is tampering with the upper beaver dam under the power lines,” said a commission member. “It looks like branches have been pulled from the base of the dam, so water is flowing through.” The commission asked the Ayer Public Spirit to warn the public there is a $25,000 fine for tampering with a beaver dam. On July 11, 2011, a violent dam burst sent 19 million gallons of water rushing downstream. The force of the torrent washed away the underpinnings of Oakridge Drive and tons of sediment and roadway material washed into the

85-acre Flannagan Pond. A department of fisheries and wildlife Highway assistant foreman said May 14 he saw "a new trail going down right to the dam made by someone using a four-wheeler" that was not there last time he checked in March. Source: http://www.nashobapublishing.com/ayer_news/ci_20653484/alarm-over-evidence-dam-tampering

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168